Data Controllers for Shared Records

Contents

Purpose 1
Data Controller Issues 1
Joint Data Controllers and Data Controller in Common 2
Data Processors 3
Who are the Data Controllers for NHS Patient Data? 4
Appendix 1: Checklist of Key Issues 8
Appendix 2: Data Controller Responsibilities and Data Processor Requirements 12

Purpose

This guidance aims to support the development of integrated digital care records (IDCRs) by considering a number of issues faced by organisations and communities when sharing information for care. A checklist of key considerations for a care community planning to share information is provided at Appendix 1. The high level requirements[1] that organisations, those who process data on their behalf, and the care record IT systems they employ, must satisfy are listed in Appendix 2. This guidance will be of interest to IG staff, Caldicott Guardians and those involved in projects supporting integrated care.

Data Controller Issues

The Data Protection Act 1998 sets out clear responsibilities that must be met by data controllers even though it may not always be straightforward to determine who they are in a shared record environment. Organisations processing data about identifiable individuals will be either a data controller for that data or a data processor. The term 'processing' refers to any activity involving the data: holding, viewing, sharing, deletion etc. Data sharing may involve an actual transfer of recorded data or simply relate to enabling information to be viewed by a third party.

[1] These requirements are derived from the Data Protection Act 1998, common law confidentiality requirements and the Health and Social Care (Safety and Quality) Act 2015

A data controller:

- Is an individual or body with a legal identity (e.g. NHS Trusts, CCGs, GP Practices, Local Authorities)
- Determines the purposes for which personal data will be processed and/or
- Determines the way that the data is processed

It is important to establish whether someone is a data controller because it is data controllers who are required to comply with the Data Protection Principles and meet the other obligations imposed by the Data Protection Act. The Information Commissioner's view is that understanding what data will be used for is paramount in deciding who is a data controller. Disclosing information to another body or permitting another body to access information is not in itself sufficient to make the other body a data controller for that information (see the section on data processors below). However, if the other body processes the information in a meaningful way, e.g. stores it or makes use of it for their own purposes, they will be a data controller for that information.

Note that organisations do not have any legal right to access confidential personal information (e.g. care records) simply by virtue of being a data controller – consent or some statutory provision will still normally be required. The Data Protection Act provides clear rules for data controllers and conditions that must be satisfied for processing of personal data to be lawful. Confidentiality law in effect provides an additional set of conditions that data controllers must satisfy when the personal data concerned has the quality of confidentiality.

Joint Data Controllers and Data Controller in Common

The determination of the purposes for which, and the manner in which, any personal data are, or are to be, processed does not need to be exclusive to one data controller. Authority to make such determinations may be shared with others. The Data Protection Act recognises two models of shared authority:

1. Joint data controllers, and
2. Data controllers in common.

"Joint" covers the situation where the determination is exercised by data controllers acting together, typically with written data controller agreements[2] setting out the purposes for processing, the manner of processing and the means by which joint data controller responsibilities will be satisfied. The participation of the parties may take different forms and need not necessarily be equally shared across all aspects of the processing. Their contributions may be sequential or simultaneous and their liability if something goes wrong may differ. The Information Commissioner usually has little difficulty in determining the responsible data controller when something does go wrong – it is a matter of fact who actually made decisions about processing.

"In common" is where data controllers share a pool of personal data, often disclosing data to each other but with each processing the data independently of the other(s). As with 'joint' arrangements, data controllers in common should have written agreements and processes for ensuring that all data controller responsibilities are satisfied. Each needs to exercise due diligence in ensuring that all parties involved are meeting the requirements of law, e.g. seeking assurance about information governance performance, policies and processes[3].

Data Processors

The concept of 'data processor' is also relevant[4]. A data processor can be anyone (other than an employee of the data controller) who processes the data on behalf of the data controller. The Act imposes specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors. The data controller retains full responsibility for the actions of the data processor – if there is a data protection breach then the data controller remains responsible. Whether a body is a data controller or data

[2] Note that a data controller agreement is different from a data sharing agreement though it could be, and often is, incorporated within one. Essentially it sets out how data controller responsibilities will be met. https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

[3] The new EU Data Protection Regulation (GDPR) may require further guidance to be developed on these arrangements.

[4] The differences and required governance arrangements between data controllers and data processors is explained on the Information Commissioner's web site at https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

processor is a matter of fact, but when utilising a data processor a key obligation on the data controller is to ensure that the processing by the data processor is carried out under a written contract, which requires the data processor to act only on instructions from the data controller. In the absence of a written contract, a body may still be a data processor if that is what it is and the data controller will be at fault. Whether a body is a data processor or not is a matter of fact that will be apparent to an investigation – if it is not a data processor it will be a data controller in its own right and will need to meet all the requirements of the Data Protection Act.

Note that organisations do not have any legal right to access confidential personal information simply by virtue of being a data processor – consent or some statutory provision will still normally be required. Confidentiality must be maintained within and across an organisation and a data controller must have a lawful basis for sharing confidential information with a data processor.

Who are the Data Controllers for NHS Patient Data?

Each organisation has generally been the sole data controller for the personal data that it holds, whether within its IT systems or on paper or other media. Some data processor arrangements have existed, e.g. local informatics services processing data for a number of organisations, and there are a small number of examples where records have been shared for a number of years and the benefits for service users have been clearly demonstrated.

The latest generation of IT systems have been crafted specifically to facilitate information sharing to support improved patient care. The presentation of these new-shared record environments as a single record for each patient has raised the issue of whether contributing organisations are joint data controllers or data controllers in common for these records or alternatively whether information is simply being shared between different data controllers without any shared or overlapping responsibilities.

Joint data controllers are actually very rare in care settings. The effective administration of a system where true joint responsibility and accountability exists is complex. Subject to written agreements, each organisation potentially is responsible for the security of all the data held,

for its accuracy and completeness, for correcting errors etc. Each could potentially amend, delete or otherwise exert control over all the components of the record, regardless of which organisation originally recorded the data.
Data controller in common arrangements have been introduced in a number of areas, often to build shared buy in to the delivery of a project by reassuring participants that they remain in control of the data they share. However, the greater the numbers of data controllers involved, the less transparent the arrangements become and accountability for decisions can be unclear. In some cases, participating organisations may not actually be determining the purposes and the manner of the processing and may not in fact be data controllers. As mentioned earlier the ICO will determine which organisation(s) made the decisions if an incident occurs.

Two different models are considered here. The first involves information being transferred to a central hub where the collated record is then made available to participating organisations. The second involves system functionality enabling participating organisations to view a snapshot of records created in another organisation. In either model, it is necessary to consider, for each participating organisation including system suppliers:

- Is the organisation participating under a written contract that prevents it from processing data other than under the instruction of a separate data controller? If so, it is a data processor.

- If not a data processor, to what extent does the organisation determine the purposes that data are used for? To which data does this apply? At what point do they start and/or stop determining the purposes that any particular data are used for? Do they have any say over what each other does?

- Separately, consideration needs to be given to the extent that each organisation determines the way in which the data are processed. To what extent is this determined by a system supplier? To what extent does the organisation determine the way in which a partner organisation processes data?

The data controllers, when identified, will need to ensure that all data protection requirements are being effectively satisfied. This does not mean that they will each be accountable for meeting all requirements, but there needs to be a clear agreement on how requirements will be met. If responsibilities are not clearly defined and allocated there is a risk that too little will be done or differences in interpretations will lead to conflicting or competing actions resulting in failure to comply with legal obligations. A data controller agreement document will be essential where there are multiple data controllers in common.

In addition, all participating organisations will need assurance that the information they share will be kept secure and managed lawfully, regardless of whether they are data controllers. In some cases this can be addressed through a data sharing agreement but where the purpose supported is limited to care provision and each participating organisation can evidence a satisfactory information governance performance assessment then the formality of a written agreement is not always necessary or practicable e.g. a tertiary care provider may exchange information with hundreds or possibly thousands of other care providers and establishing written agreements in these circumstances is not practicable. This does not absolve such providers of their responsibility to share information responsibly and they should work within a clear policy framework and check, for example that those they send data to are meeting information governance requirements e.g. achieving appropriate performance levels using the IG Toolkit.

Information Sharing Agreements should cover:

- The assurances required by the organisations that use the system in respect of its security as individually they are unlikely to be able to specify and manage system security;
- Clarification of the legal obligations falling on each organisation using the system, including accuracy of the information they contribute;
- Clarification of expected working practices within each organisation (linked to IG Toolkit requirements)
- Reciprocal agreements in respect of additional – non-legally binding - services for patients

A good example of a reciprocal service that might be agreed locally might be the provision of a copy of information to a patient who has made a subject access request. The recipient is legally bound to provide, subject to exemptions set out in the Data Protection Act 98, a copy of the information held. There is no obligation to provide a copy of information shared by a different data controller even though it is accessible, though data controller must provide information that they are directly responsible for. However, providing a shared record has been checked in advance for potentially exempt information, there could be an agreement that this is also provided to the patient, with appropriate caveats, where this is sufficient for the patient's needs.

A checklist is provided as appendix 1 to this guidance to support health and care communities adopting a data controller in common model to develop an IDHR.

It is strongly recommended that each shared record community should establish an Information Governance Steering Group to establish effective IG arrangements for the shared record. The Steering Group should include representatives covering all the organisations party to the shared record, and we recommend the group should be chaired by a Caldicott Guardian. Products should be circulated for agreement by all parties.

When addressing the issues in the checklist, the Steering Group must consider what action must be taken in response to any question where the answer is "no". Failure to address any concerns is not an option because ineffective or weak IG controls in one organisation present a risk to the whole shared record community. It is therefore important that the Steering Group should identify what action needs to be taken, who is responsible for taking that action, and the deadline for its completion.

Appendix 2 provides a list of responsibilities, derived from the Data Protection Act but also the common law and other areas of law and sets out, at a high level, the system requirements that organisations need to develop or procure when implementing integrated digital care records.

Appendix 1: Checklist of Key Issues

What do you know about your partners?

It is strongly recommended that you and your partners in the shared record community establish arrangements to ensure the shared record environment has effective information governance. In particular, you must consider:

	Yes (✓)	No (✗)	Comments / Actions
1. Have you established a formal network of all the organisations party to the shared record?	☐	☐	
2. Are you confident that each organisation within the shared record environment complies with minimum IG standards? (E.g. Have they reached an appropriate attainment level on the NHS IGT?)	☐	☐	
3. Have you and your partners agreed arrangements for incident management and reporting?	☐	☐	
4. Have you conducted a Privacy Impact Assessment to understand risks and required mitigations?	☐	☐	

What have you told your Patients and Service Users?

It is good practice to be open with your patients and service users. You should publish a privacy notice explaining what information you record about people and the purposes for keeping and sharing records but notices alone may not be sufficient to effectively inform. If you work in a shared record environment, you may also wish to consider:

	Yes (✓)	No (✗)	Comments / Actions
1. Do the privacy notices of your organisation and your partners in the shared record community tell patients and service users about the way personal information is recorded and stored?	☐	☐	
2. Have you and your partners told patients and service users that their medical records are stored in a shared record environment?	☐	☐	
3. Do patients and service users know all of the organisations that work in the shared record environment?	☐	☐	
4. Do all patients and service users understand the circumstances in which staff working for other organisations in the shared record community might access their medical record?	☐	☐	
5. Have you and your partners in the shared record community told patients and service users about the additional privacy controls they might be able to use to restrict access to their medical records?	☐	☐	

6. Have you and your partners agreed how consent and dissent to information being included within the shared environment will be managed?	☐	☐	

What have you and your partners agreed?

You may also wish to consider establishing reciprocal agreements in respect of additional services you may supply to patients and service users. For example:

	Yes (✓)	No (✗)	Comments / Actions
1. Have you agreed with the other organisations how subject access requests will be handled? (e.g. Will each organisation in the shared record environment responding to a subject access request provide only the data it has recorded, or will it provide a copy of all information stored in the shared record environment?)	☐	☐	
2. Have you established a process for managing and resolving issues relating to data quality or accuracy or patient/service user concerns about shared record content?	☐	☐	
3. Have you agreed a process with the other organisations in the shared record environment for managing service user objections to the processing of personal data about them?	☐	☐	

4. Have you agreed a process with the other organisations in the shared record environment to manage third party requests for access to personal records?	☐	☐	

What have you agreed with your system supplier?

It is essential that you agree a contract with your system supplier that ensures you have effective control of any personal information it is processing on your behalf. Key considerations:

	Yes (✓)	No (✗)	Comments / Actions
1. Do you (and your partners in the shared record environment) have a written contract with your system supplier?	☐	☐	
2. Is it clear that your system supplier can act only under instruction from you (and your partners)?	☐	☐	
3. Does your system supplier understand that it cannot extend access to the shared record environment to new organisations without your prior approval (and that or your partners)?	☐	☐	

Appendix 2: Data Controller Responsibilities and Data Processor Requirements

	Data Controller Responsibilities	Data Processor & System Requirements
1	To ensure that data subjects have access to fair processing information that tells them: • Who their personal data will be shared with • The purposes that their personal data will be used for • The choices they have and how to exercise those choices	Data Processor to provide all data controllers with details of the third parties with which personal data has been disclosed
2	To decide whether or not to collect personal data	System must support authorised data collection and prevent unauthorised collection
3	To ensure there is a lawful basis for collecting the data	N/A (Data Controller responsibility)
4	To decide which items of personal data to collect	System must support data controllers to enable all necessary data to be recorded in appropriate formats
5	To decide which individuals to collect data about	System must support authorised data collection
6	To decide whether subject access and other individual rights apply	System must support data controllers to consider and meet individual rights e.g. subject access
7	To determine the purpose(s) that the data will be used for	System must enable the data controller to undertake activities specified in the data processor contract and prevent

		personal data being processed for other purposes
8	To decide whether to disclose personal data	System must not permit personal data to be disclosed without the data controllers authorisation, but must facilitate authorisation process where appropriate
9	To decide who to disclose personal data to	System must enable the data controller to choose whether or not to disclose personal data to any particular recipient and to select one recipient but not another
10	To decide what personal data to disclose – proportionality, necessity, granularity	System must enable the data controller to determine which data items should be disclosed to each recipient or potential recipient. Data controllers may elect to utilise a consistent data specification if one is available e.g. which data items to share with a care home

11	To share personal data when required by statute e.g. the duty to share introduced by the Health & Social Care (Safety & Quality) Act 2015 and the requirement to include the NHS Number also introduced by that Act	To enable required personal data to be shared when authorised by the data controller with any third party where this is required by law (and to be developing any necessary functionality where this currently does not exist)
12	To ensure there is a lawful basis for disclosing personal data with the data processor and with other data controllers	N/A (Data Controller responsibility)
13	To determine how long personal data should be retained	System must support national minimum retention requirements and facilitate compliance with the 20 year rule
14	To authorise any amendments to the personal data held	System must not permit any amendments to personal data that have not been specifically authorised by the data controller and should facilitate data to data controller contact and joint resolution where there is record confusion or duplication
15	To choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out	Data Processor must provide reasonable assurances as specified in the data processor contract

16	To take reasonable steps to ensure data processor compliance with those security measures	Data Processor must facilitate an audit of security measures by the data controller of an appointed agent and must make the results of such audits available to all data controllers using the system
17	To restrict access to confidential personal data on a need to know basis and to system functionality on a role/position basis	Where data processors are also the system suppliers for the data controller's IT system they must ensure that the available controls facilitate the data controller meeting relevant requirements
18	To ensure that data processing is carried out under a contract — which is made or evidenced in writing, and under which the data processor is to act only on instructions from the data controller	Data Processor to provide assurance as specified in the data processor contract that all processing of a data controller's personal data has complied with this requirement and that no processing has been undertaken without instruction